DAVID JAO, University of Waterloo

Isogeny-based Cryptography

Cryptosystems based on isogenies between elliptic curves have recently been proposed as plausible alternatives to traditional public-key cryptosystems. These systems are of particular interest because they are conjectured to be resistant to attacks by quantum computers. We survey the existing constructions of isogeny-based public-key cryptosystems and describe the fastest known attacks against them. In the case of ordinary curves, we present an algorithm for evaluating isogenies, whose running time is provably subexponential under GRH. For supersingular curves, we propose a public-key cryptosystem based on pairs of isogenies over a curve with disjoint kernels, having performance competitive with standard cryptosystems, and describe our recent performance optimizations.

Joint work with A. Childs, L. De Feo, J. Plût, and V. Soukharev.